Safety critical function monitoring of control systems for process control applications has separate unit

Patent number:	DE19857683
Publication date:	2000-06-21
Inventor:	WRATIL PETER (DE)
Applicant:	WRATIL PETER (DE)
Classification:	
- international:	G05B19/406; G05B23/02
- european:	G05B19/042S; G05B19/05S; G05B23/02
Application number:	DE19981057683 19981214
Priority number(s):	DE19981057683 19981214

Abstract of **DE19857683**

The system has a main controller (1) bus coupled to different processors (11,12) via a number of decentralized data receivers (4-10). Connected to the bus is a watchdog unit that monitors safety critical parameters. The watchdog controller has embedded software that allows functions and actions to be selected.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 57 683 A 1**

(51) Int. Cl.[7]:
G 05 B 19/406
G 05 B 23/02

(21) Aktenzeichen: 198 57 683.8
(22) Anmeldetag: 14. 12. 1998
(43) Offenlegungstag: 21. 6. 2000

DE 198 57 683 A 1

(71) Anmelder:
Wratil, Peter, Dr., 21224 Rosengarten, DE

(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Sicherheitsüberwachung von Steuerungseinrichtungen

(57) Es wird ein Verfahren zur Erhöhung der Sicherheit bei Automatisierungseinrichtungen beschrieben. Das Verfahren ist derart ausgelegt, daß man übliche Steuerungseinrichtungen mit dezentralen Peripheriegeräten in Bezug auf sicherheitsrelevante Vorgänge und Abläufe redundant überwacht und damit gehobenen Sicherheitsanforderungen zum Schutz von Leben und Gesundheit von Personen oder Maschinenteilen gerecht wird. Bei dem vorgestellten Verfahren wird eine weitreichende Trennung zwischen dem Steuerungssystem und der Sicherheitseinrichtung erreicht, so daß eine nachträgliche Installation in einfachster Form möglich wird. Zusätzlich ist man in der Lage, sowohl das Steuerungssystem als auch die Sicherheitseinrichtung unabhängig zu programmieren und zu prüfen.

DE 198 57 683 A 1

BUNDESDRUCKEREI 04.00 002 025/210/1 14

Safety critical function monitoring of control systems for process control applications has separate unit

Description of DE19857683

Die Erfindung bezieht sich auf ein Verfahren zur Sicherheitsüberwachung von Steuerungseinrichtungen.

Steuerungseinrichtungen werden nach dem heutigen Stand der Technik überall dort eingesetzt, wo Prozesse, Abläufe oder sonstige elektromechanische Einrichtungen zu steuern, regeln, überwachen oder zu visualisieren sind. Im engeren Sinne verwendet man hierzu oftmals speicherprogrammierbare Steuerungen oder Mikrorechner. Typische Anwendungsgebiete sind Automatisierungsinseln, Fertigungsstrassen, Bearbeitungszentren oder chemische Einrichtungen.

Nicht selten enthalten diese vorher genannten Prozesse sicherheitsrelevante Abläufe, die eine Gefährdung für Personen oder Teile der Maschine darstellen. Von den fehlerhafte Zuständen der Steuerung gehen dann extreme Gefahren aus, die unbedingt von Personen oder sonstigen Einrichtungen fern zu halten sind. Beispiele hierfür sind unkontrollierte Bewegungen von Robotern, vorzeitiges Bewegen von Dreh- oder Fräseinrichtungen, ungewollte Beschleunigungen oder falsche Drehzahlen von Rotationseinrichtungen oder verzögertes Abschalten von Heiz- oder Dosierprozessen bei chemischen Anlagen. Die Ursachen dieser fatalen Fehler sind vielfältig. Zumeist liegt aber ein Programmierfehler, ein unkontrolliertes Verhalten durch elektromagnetische Einflüsse oder eine sonstige Störung vor, die den Prozess in eine nicht definierte Situation bringt.

Diese Fehlerarten sind in der Literatur (insb. in Normungswerken, vergl. DIN 19251) hinreichend beschrieben. Gleichfalls stellt die Norm bereits Konzepte vor, wie man derartige Fehler erkennt und eliminiert (z. B.: DIN V 0801). Ferner bieten verschiedene Hersteller von Steuerungseinrichtungen bereits vollständige Lösungen an, die für sicherheitsrelevante Einrichtungen (wie vorgestellt) zu verwenden sind (siehe Produktangebote Siemens (115/155F) oder Produkte der Hersteller Pilz und Hima).

Alle bekannten Lösungen basieren darauf, dass man entweder die gesamte Steuerungseinrichtung oder Teile der Steuerungseinrichtung redundant auslegt. So entsteht ein Gesamtsystem, das man bei allen sicherheitsrelevanten Komponenten entweder doppelt oder dreifach projektiert werden muss. Insbesondere stellt die Sicherheitseinrichtung bei einer derartigen Steuerung einen festen Bestandteil des Gesamtsystems dar. Jede Änderung oder Anpassung an den Prozess muss sorgsam (im Hinblick auf die Sicherheitsfunktion) durchgeführt werden, da auch nichtsicherheitsrelevante Hard- oder Softwarekomponenten einen Einfluss auf die Sicherheitseinrichtung haben können. Im schlimmsten Fall könnte sogar die Änderung eines Parameters zum Absturz der Sicherheitseinrichtung führen.

Bereits in der Vergangenheit war man daher stets bemüht, reine Steuerungsabläufe von sicherheitsrelevanten Vorgängen zu trennen (siehe auch Patent DE 35 02 387 oder Fachartikel "SPS in der Sicherheitstechnik", SPS-Magazin, Feb./März 1990) Nach wie vor stellen auch diese Konzepte Verfahren dar, die zwar ohne Verdopplung der Hardware auskommen, aber die sicherheitsrelevante Funktion in der Gesamtprojektierung der Steuerung benötigen.

Der Erfindung liegt die Aufgabe zu Grunde, die Steuerungseinrichtung und die Sicherheitsfunktion vollkommen zu trennen. Mit der Erfindung wird es möglich, den Steuerungsteil vollständig vorher aufzubauen, zu testen und in Betrieb zu nehmen. Die sicherheitsrelevanten Komponenten lassen sich dann nachträglich hinzufügen, ohne die Steuerungsfunktion zu ändern. Auch nach der Installation beider Systeme (Steuerungseinrichtung und Sicherheitssystem) lassen sich Steuerungsfunktionen ändern, hinzufügen oder heraustrennen, ohne dass die Sicherheitsfunktion davon betroffen ist. Insbesondere besteht die Möglichkeit, alle Sicherheitsverknüpfungen im einzelnen unabhängig zu prüfen.

Diese Aufgabe wird erfindungsgemäss durch die kennzeichnenden Merkmale des Anspruchs 1 gelöst, während die weiteren Ansprüche (2-10) vorteilhafte Ausprägungen des Verfahrens darstellen.

In Fig. 1 ist die Funktionsweise des zu Grunde liegenden Verfahrens dargestellt. Hierbei besteht das Automatisierungssystem aus einer Steuerung, einem Bus-System und mehreren dezentralen Komponenten, die den Prozess steuern oder überwachen. Damit stellt die Fig. 1 eine typische Einrichtung dar, die (ohne die grau hinterlegten Komponenten) für alle nichtsicherheitsrelevanten Systeme geeignet sind. Die Anordnung entspricht dem heutigen Stand der Technik.

Im Detail steuert oder regelt die Steuerung (1) den gewünschten Prozess. Über das angeschlossene Bus-System (3) holt sie Daten vom Prozess (11, 12) oder gibt sie Daten zum Prozess aus. Die dezentralen Einheiten (4-10) empfangen alle Daten vom Bus-System (3) oder stellen dem Prozess (11, 12) ihre Daten zur Verfügung. Damit sind die dezentralen Einheiten nur vorgelagerte Ein-/Ausgabe-Baugruppen, die ohne ein Bus-System als Peripheriebaugruppen in der Speicherprogrammierbaren Steuerung zu finden sind. Die Steuerung (1) enthält ein

Programm (Software) das all[redacted]tsicherheitsrelevanten Vorgänge steuert oder reg[redacted]rner enthält sie bereits in ihrem Programm auch die log[redacted]n Funktionen für die Sicherheitsverknüpfungen, die [redacted] sicherheitsrelevante Vorgänge notwendig sind. So enthält beispielsweise der Prozess (11) keine aber der Prozess (12) sicherheitsrelevante Vorgänge bei denen Bewegungen erfolgen, die eine Gefahr für Mensch oder Maschine darstellen (13). Obwohl die Steuerung (1) die notwendige Logik für die Sicherheitsanforderung enthält, kann sie im Fehlerfall nicht einwandfrei reagieren, da entweder sie selbst oder eine ihrer dezentralen Einheiten fehlerbehaftet sein kann, diese aber nicht kontrolliert werden. Das Steuerungssystem ist damit nicht in der Lage, einen Fehler abzuwehren, da jegliche Fehlererkennung fehlt.

Entsprechend der Aufgabe des Patents nach Anspruch 1 werden zur Erreichung der sicheren Fehlererkennung und zur Prozessabschaltung die grau hinterlegten Komponenten hinzugefügt. Die Überwachungseinheit (2) wird in der Funktion eines Hörers (Listener) an den Bus angeschlossen. Sie braucht damit nicht von der Steuerung berücksichtigt zu werden, da sie nur passiv sich der Daten des Bus-Systems (3) bedient. Die Überwachungseinheit (2) ist über die auf dem Bus laufenden Daten über alle Zustände und Abläufe im Prozess und insbesondere über die Zustände der Prozessgrössen informiert. Im Prinzip ist sie damit in der Lage, die sicherheitsrelevanten Zustände zu überprüfen. Zur Bewältigung dieser Aufgabe enthält sie ein einfaches Programm dass nur die Sicherheitsfunktionen als Logik überwacht (z. B.: Gitterkontrolle, Anlaufüberwachung, Endschaltertest, usw.). Im Fehlerfall der Steuerung (1) kann damit die Überwachungseinheit (2) geeignete Massnahmen ergreifen. Diese Fehlererkennung funktioniert jedoch nur dann, wenn die Steuerungseinheit (1) als Verursacher fungiert. Fehler in den dezentralen Einheiten oder im Prozess werden von beiden Einheiten (Steuerungseinheit (1) oder Überwachungseinheit (2)) nicht registriert. Eine vollständige Kontrolle gelingt daher nur mittels spezieller dezentraler Einheiten, die ihre eigene Funktion oder sogar die Sensorik im redundant Prozess abfragen. Entsprechend des Anspruchs 1 gehören zum Verfahren auch dezentrale Einheiten, die selbst Sicherheitsanforderungen genügen. Hierzu gehört insbesondere die Überwachung der eigenen Funktion und die Sicherheitsabschaltung im Fehlerfall (bei Ausfall des Bus-Systems (3) oder bei fehlerhaften Ein- oder Ausgabe).

Die Überwachungseinheit (2) erkennt somit eindeutig einen Fehler, sofern er im sicherheitsrelevanten Programm als Logik hinterlegt ist. Es bleibt der speziellen Projektierung überlassen, in welcher Form eine geeignete Sicherheitsabschaltung erfolgt. Im einfachsten Fall kann die Überwachungseinheit (2) das Bus-System (3) unterbrechen oder kurzschliessen. Damit unterbindet sie die Datenübertragung und die dezentralen Einheiten (7, 9) fallen in einen sicheren Zustand. Denkbar ist aber auch ein gezieltes Abschalten der Stromversorgung oder ein langsames Herunterfahren des Prozessablaufs.

Safety critical function monitoring of control systems for process control applications has separate unit

Claims of **DE19857683**

1. Verfahren zur Sicherheitsüberwachung von Steuerungseinrichtungen, bei denen Speicherprogrammierbare Steuerungen oder Mikrorechner über ein Bus-System dezentrale Einheiten ansprechen, die einen Prozess sowohl im sicherheitsrelevanten als auch im nichtsicherheitsrelevanten Bereich regeln, steuern oder überwachen, dadurch gekennzeichnet, dass zur Realisierung der Sicherheitsanforderung eine Überwachungseinheit (2) hinzugefügt wird, die entweder ausschliesslich oder vorwiegend die sicherheitsbehafteten Funktionen des Prozesses (12) mit der notwendigen Logik zur Überwachung gefahrbringender Abläufe oder Bewegungen (13) hinzugefügt wird, die selbst nur über das Bus-System (3), welches als Standard erhalten bleibt und keinerlei Zusatzfunktion bedarf, eine Hörer-Funktion erhält und damit zusätzlich zum Gesamtprozess adaptierbar ist, diese mit sicherheitsgerichteten dezentralen Einheiten (7, 9) kommuniziert und parallel zum Gesamtprozess alle Sicherheitsfunktionen überwacht und nur im Fehlerfall über die dezentralen Einheiten (7, 9) oder sonstigen Sicherheitseinrichtungen den sicheren Maschinen- bzw. Anlagenzustand herbeiführt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungseinheit (2) über eine in der Programmiersprache festgelegten Logik verfügt, die entweder ausschliesslich oder vorwiegend Sicherheitsvorgänge überwacht und damit redundant zur Gesamtsteuerung arbeitet.

3. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, dass die Überwachungseinheit (2) auch nach der Funktionskontrolle des nicht redundanten Steuerungssystems mit ihren für die Sicherheit notwendigen Abschaltfunktionen adaptierbar ist und durch ihre Sicherheitsfunktion der geforderte Grad an Sicherheit projektiert werden kann.

4. Verfahren nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, dass die Überwachungseinheit (2) und die sicherheitsgerichteten dezentralen Einheiten (7, 9) deaktiviert werden können, ohne die einkanalige Steuerungsfunktion zu beeinträchtigen.

5. Verfahren nach den Ansprüchen 1 bis 4, dadurch gekennzeichnet, dass durch eine bustechnische Mithörfunktion der Überwachungseinheit (2) keine Rückwirkung auf den eigentlichen Steuerungsprozess entsteht, so dass eine weitgehende Trennung zwischen der Hard- und Software des nicht redundanten Steuerungssystems und der Sicherheitsüberwachung ermöglicht wird.

6. Verfahren nach den Ansprüchen 1 bis 5, dadurch gekennzeichnet, dass die Überwachungseinheit (2) über den normalen Datenverkehr des Bus-Systems (3) der Steuerungseinheit (1) alle notwendigen Zustände und Funktionen erhält, die zur Überwachung des nicht redundanten Steuerungssystems notwendig sind.

7. Verfahren nach den Ansprüchen 1 bis 6, dadurch gekennzeichnet, dass es an Standardbussysteme ohne Sicherheitsprotokollerweiterung adaptierbar bzw. einbindbar ist.

8. Verfahren nach den Ansprüchen 1 bis 7, dadurch gekennzeichnet, dass die dezentralen Einheiten, die sicherheitsrelevante Funktionen erfassen und ansteuern, selbst ihre Funktion überwachen, möglicherweise Sensoren oder Aktoren redundant überwachen und bei Ausfall einer Funktion, beispielsweise bei Ausfall der Bus-Funktion, in den sichern Zustand schalten, der keine Gefahr mehr für Mensch oder Maschine darstellt.

9. Verfahren nach den Ansprüchen 1 bis 8, dadurch gekennzeichnet, dass die Überwachungseinheit (2) in einer von dem nicht redundanten Steuerungssystem unabhängigen Programmier- und Parametriersprache in ihren Sicherheitsfunktionen generiert werden.

10. Verfahren nach den Ansprüchen 1 bis 9, dadurch gekennzeichnet, dass die Überwachungseinheit (2) neben der Überwachungsfunktion auch die Bedienung und Programmierung mittels eines integrierten Mensch-Maschinen-Interfaces erlaubt.

Nummer: DE 198 57 683 A1
Int. Cl.⁷: G 05 B 19/406
Offenlegungstag: 21. Juni 2000

Fig. 1